УДК 004.451.36:681.5

РОЗРОБЛЕННЯ СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ ДО ДОКУМЕНТІВ В АСДО ДЛЯ ПОЛІГРАФІЧНИХ ВИДАВНИЦТВ

В. І. Сабат, В. В. Мацюк, М. М. Мусійовська, Н. І. Каневська

Українська академія друкарства,
вул. Під Голоском, 19, Львів, 79020, Україна

Проаналізовано основні засоби управління доступом до документів, на основі чого запропоновано систему управління доступом в автоматизованих системах документообігу (АСДО) для поліграфічних видавництв. Визначено, що для поліграфічних видавництв необхідною умовою для функціонування системи управління доступом до документів є встановлення рівнів таємності документів, впровадження засобів двофакторної ідентифікації користувачів, розроблення процедур моніторингу та правил роботи з документами. Запропоновано загальний принцип роботи системи захисту документів в АСДО для поліграфічних видавництв.

Ключові слова: *системи управління доступом до документів, автоматизовані системи документообігу, методи ідентифікації та аутентифікації осіб.*

Постановка проблеми. Розроблення системи управління доступом до таємної інформації, яка міститься в документах, є основним завданням надійного функціонування АСДО. Від того, як буде сформований кожен документ на етапі його створення, який захист обереться для запобігання несанкціонованим спробам його відкриття чи модифікації, який механізм обереться для ідентифікації осіб і надання їм прав доступу, певною мірою залежить робота не тільки системи документообігу, а й усього підприємства. Тому виникає проблема у створенні таких засобів та методів доступу до документів, які б забезпечили рівень захисту інформації в них і дозволили контроль виконання документів на усіх етапах роботи з ними.

Аналіз останніх досліджень та публікацій. Виконані дослідження з цієї тематики присвячені створенню моделей систем управління повноваженнями в системах захисту інформації [1], розробленню структури управління повноваженнями [2, 3], методів формального опису систем управління повноваженнями на основі використання математичної логіки [4], методам захисту документів в системах документообігу [5]. Водночас недостатньо уваги приділено розробленням системи управління доступом до документів в АСДО.

Мета статті орієнтована на розроблення системи управління доступом до документів в АСДО для поліграфічних видавництв і вибору оптимальних методів захисту документів.

Виклад основного матеріалу дослідження. Для нормалізації роботи автоматизованої системи документообігом (АСДО) у будь-якій організації чи на під-

приємстві необхідно встановити правила та процедури безпеки роботи з документами. Для цього необхідною умовою є забезпечення відповідними службами безпеки системи управління доступом до АСДО. Служба безпеки, яка має наявний штат працівників підрозділу надання доступу до конфіденційної інформації, співпрацює з адміністрацією та іншими службами, наприклад з відділом кадрів, інформаційним відділом та підрозділами, де функціонують документи, розробляє для кожного працівника рівень доступу до документів. Отже, розробляється система ідентифікації усіх суб'єктів в АСДО і, згідно з їхнім рівнем кваліфікації та службовим становищем, пов'язаним з роботою з секретними документами, надається відповідний рівень доступу.

Особливо це стосується нових працівників, які влаштовуються на роботу, і відповідно до процедур, прописаних у політиці безпеки підприємства, вони повинні бути ознайомлені з правилами системи безпеки і роботи з документами, а також мають бути обізнаними про відповідальність за порушення правил безпеки, особливо, коли це призведе до збитків в організації. Свою згоду про те, що вони ознайомлені з процедурами політики безпеки і рівнем своїх повноважень та обов'язків нові працівники засвідчують своїм підписом.

Проте на початковому етапі розроблення системи управління доступом необхідно визначити, що саме вважається секретним для будь-якої організації. Такий аналіз насамперед ґрунтується на визначенні рівня ризику та втрат в разі непередбачених інцидентів та атак на організацію. До таких атак потрібно зарахувати атаку доступу до інформації, що міститься в документах. Вона може бути здійснена як ззовні, так і всередині організації за допомогою проникнення зловмисника до ресурсів АСДО або підкупу службовців організації.

Отже, після визначення рівня ризику, усіх вразливостей та загроз визначається рівень секретності документації або, інакше кажучи, рівень таємності документів. На деяких підприємствах цей рівень не перевищує позначки 3, наприклад можуть бути документи загального використання — це перший рівень, доступ до таких документів надається практично усім суб'єктам поліграфічних видавництв (ПВ). Другий рівень — це конфіденційна інформація, або для службового користування, право на читання та використовування такої інформації матимуть лише ті службовці, які працюють з вказаними документами, наприклад відділ бухгалтерії, який нараховує заробітні плати усім суб'єктам ПВ, для інших службовців така інформація може бути конфіденційною. Третій рівень таємності, чи доступу до документів, які можуть мати назву як надзвичайно секретні документи, або документи для закритого користування. Така інформація доступна лише особам, які розробляють політику безпеки в ПВ, а також адміністрації чи власникам підприємства, які мають право змінювати цю політику безпеки [6].

До важливих етапів розроблення системи доступу також належать процедури та правила визначення факторів ідентифікації користувачів під час роботи з документами. Система доступу має гарантувати захист таємних документів від несанкціонованого доступу до них. Тому необхідно впровадити в АСДО сучасні методи ідентифікації та аутентифікації усіх суб'єктів ПВ.

Згідно з класичними підходами до розроблення систем безпеки встановлюються такі три фактори ідентифікації користувача в системі безпеки:

1. Те, що ви знаєте;
2. Те, що ви маєте;
3. Те, ким ви є.

У більшості випадків використовують лише один рівень захисту, а саме «те, що ви знаєте», тобто пароль. Використання паролів в організації необхідно прописати в спеціальних процедурах, які входять також в політику безпеки. Крім довжини пароля і необхідного набору символів (звичайних літер, прописних, цифр тощо), в політиці безпеки також визначають період оновлення паролів доступу до документів. Служба безпеки відповідальна за дотримання цих правил для гарантії та запобігання зовнішніх атак, пов'язаних зі «слабкістю пароля захисту».

При створенні нового документа система використання та надання паролів передбачає контроль за дотриманням вищевказаних процедур і в разі недостатнього їх виконання видає попередження про те, що пароль недостатньо захищений від злому. Паролі для відкриття захищених документів можуть надаватися службовцям відповідною службою безпеки або уповноваженим на це її представникам. Можуть бути встановленні паролі лише на читання документів із забороною їх редагування і внесення змін. Це особливо важливо, коли з документами працює група співробітників і будь-яка модифікація документа може призвести до непоправних наслідків. Також введення службовцями неправильного паролю автоматично фіксується у спеціальних журналах виявлення інцидентів та можливих атак і обробляється системним адміністратором чи працівниками служби безпеки та доступу до інформації в АСДО.

У деяких ПВ може використовуватися двофакторна ідентифікація для захисту документів. Згідно з класичним принципом, окрім того що ви знаєте пароль чи пін-код, необхідно мати ще картку, — за аналогією з банкоматом, в якому теж використовується дворівневий захист для входу в систему видачі готівки або здійснення будь-яких транзакцій. Двофакторна ідентифікація використовується тоді, коли необхідно обмежити доступ до надзвичайно секретних документів. Наприклад, якщо йдеться про великі замовлення або секретну інформацію для системних адміністраторів мереж, то такі електронні документи, окрім пароля, можуть апаратно зашифровуватися і для зчитування інформації з них необхідно мати ключ або чіпові картки чи флеш-карти, які слугують другим рівнем захисту доступу до документів. Для цього в політиці безпеки прописуються алгоритми шифрування та згідно з міжнародними стандартами розроблення систем безпеки встановлюється система захисту для такої інформації та відповідних документів.

Третій рівень захисту документів — «те, ким ви є практично» у ПВ майже не використовується. Може бути введений у банківських установах або в секретних організаціях військового типу. Цей рівень захисту, окрім пароля, — «те, що ви знаєте», картки — «те, що ви маєте» ще перевіряє «те, ким ви насправді є». Тобто, говорячи словами спеціалістів із служби безпеки, відбувається аутентифікація особи. У таких випадках використовують біологічні методи зчитування інформації, наприклад відбитки пальців, знімок сітківки ока, розпізнавання обличчя тощо [7].

Ідентифікація і аутентифікація застосовуються в системі управління доступом до файлів документів в АСДО, що забезпечує конфіденційність і цілісність цих файлів. Ідентифікація і аутентифікація дуже важлива для роботи механізмів шифрування і цифрових підписів. В цьому випадку ідентифікаційні дані передаються віддаленому користувачу, який підтверджує свою достовірність на локальному рівні, а потім ці відомості доставляються в потрібне місце. На рис. 1 показаний процес ідентифікації за допомогою цифрового підпису під час відправки документа в АСДО.

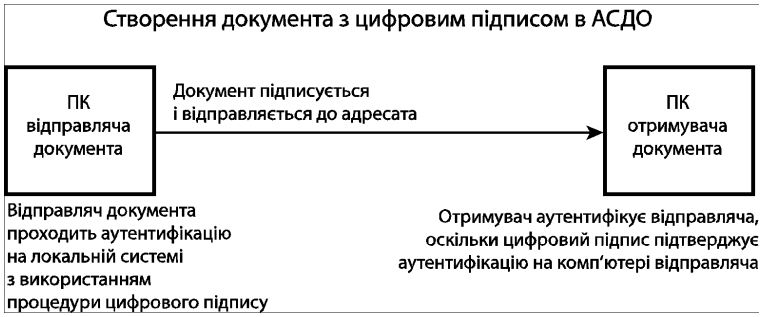

Рис. 1. Процес ідентифікації за допомогою цифрового підпису в АСДО

Відправник спочатку підтверджує свою достовірність, використовуючи механізм захисту підпису на своєму локальному комп'ютері. Потім локальний комп'ютер відправляє повідомлення, підписане цим цифровим підписом. Користувач, що отримує повідомлення, використовує цифровий підпис як доказ того, що відправник є автором повідомлення.

Механізм ідентифікації і аутентифікації — це ключ до інших служб безпеки. Якщо він дає збій, то їх надійна робота буде під загрозою.

Для того щоб розробити систему управління доступом на ПВ, як вже вказувалось раніше, необхідно:

1. Визначити секретну інформацію і поділити документи на стадії їх створення і в базі даних АСДО на рівні таємності.

2. Розробити базу даних користувачів, правила їх ідентифікації та аутентифікації в АСДО і надати кожному суб'єкту ПВ рівень доступу до документів згідно з рівнем їх таємності.

3. Розробити інструкції та правила роботи службовців з документами згідно з процедурами, описаними в політиці безпеки ПВ.

4. Службам безпеки систематично проводити моніторинг системи захисту АСДО на наявність вразливих місць та при виникненні інцидентів можливість оперативного відновлення її роботи.

Загальний принцип роботи системи захисту документів в АСДО подано на рис. 2.

Окрім формування бази документів АСДО з рівнями їх таємності, також необхідно передбачити процедури ведення баз даних користувачів, їх ідентифікації в

системі, введення нового користувача і зміни рівня доступу згідно з правилами безпеки. Таємність документів може бути обмежена періодом їх використання і виконання тих чи інших управлінських дій, після чого документ може втрачати свій статус таємності або передаватись в архів через базу документів АСДО. Також для будь-якого користувача може зрости рівень доступу, що обумовлюється адміністрацією та службою безпеки. У політиці безпеки також передбачаються процедури звільнення працівника, особливо у тих випадках, якщо він мав високий рівень доступу до інформації. Тоді служба доступу заздалегідь повинна провести необхідні заходи для зміни правил ідентифікації згідно із процедурами доступу до документів в АСДО.

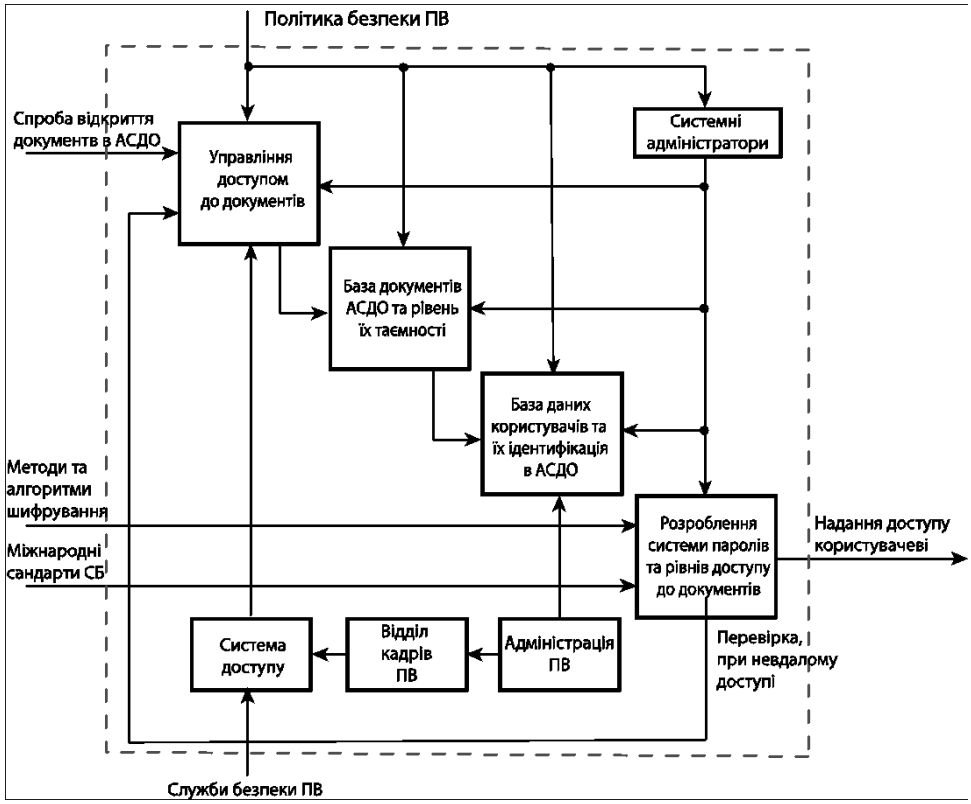

Рис. 2. Загальний принцип роботи системи захисту документів в АСДО

Висновки. Розроблення систем управління доступом до документів в АСДО для ПВ потребує не тільки кваліфікованих спеціалістів в галузі безпеки, а й залученні всіх служб та підрозділів видавництва до реалізації цього процесу. Подальше функціонування системи документообігу залежатиме від дотримання користувачами усіх процедур та правил, описаних в політиці безпеки щодо роботи з документами, а також від періодичного моніторингу роботи АСДО з боку системних адміністраторів та служб безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дурняк Б. В., Сабат В. І., Шведова Л. Є. Управління повноваженнями в системах захисту інформації : монографія. Львів : УАД, 2016. 148 с.
2. Розробка структури системи управління повноваженнями / Дурняк Б. В., Сабат В. І., Шведова Л. Є., Білак Ю. Ю. *Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України.* 2011. Вип. 58. С. 192–200.
3. Дурняк Б. В., Сабат В. І., Шведова Л. Є. Структура системи управління повноваженнями. XXX науково-технічна конференція «Моделювання» : тези конференції (12–13 січня 2011 р.). Київ, 2011. С. 60–61.
4. Дурняк Б. В., Сабат В. І., Шведова Л. Є. Методи формального опису систем управління повноваженнями на основі використання математичної логіки. *Збірник наукових праць ІПМЕ ім. Г. Є. Пухова НАН України.* 2010. Вип. 57. С. 267–275.
5. Сабат В. І. Методи захисту документів в системах документообороту. *Комп'ютерні технології друкарства.* 2004. Вип. 12. С. 297–305.
6. Дурняк Б. В., Сабат В. І., Шведова Л. Є. Загальна організація використання інформаційних засобів для створення системи управління повноваженнями. *Зб. наук. пр. ІПМЕ НАН України.* 2011. Вип. 59. С. 200–207.
7. Гуцалюк М. В. Ідентифікація фізичних осіб як протидія організованій злочинності та тероризму. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* Київ, 2005. № 11. С. 36–48.

REFERENCES

1. Durniak, B. V., Sabat, V. I., & Shvedova, L. Ye. (2016). Upravlinnia povnovazhenniamy v systemakh zakhystu informatsii. Lviv : UAD (in Ukrainian).
2. Durniak, B. V., Sabat, V. I., Shvedova, L. Ye., & Bilak, Yu. Yu. (2011). Rozrobka struktury systemy upravlinnia povnovazhenniamy: Zbirnyk naukovykh prats IPME im. H. Ye. Pukhova NAN Ukrainy, 58, 192–200 (in Ukrainian).
3. Durniak, B. V., Sabat, V. I., & Shvedova, L. Ye. (2011). Struktura systemy upravlinnia povnovazhenniamy. XXKh naukovo-tekhnichna konferentsiia «Modeliuvannia» : tezy konferentsii (12–13 sichnia 2011 r.). Kyiv, 60–61 (in Ukrainian).
4. Durniak, B. V., Sabat, V. I., & Shvedova, L. Ye. (2010). Metody formalnoho opysu system upravlinnia povnovazhenniamy na osnovi vykorystannia matematychnoi lohiky: Zbirnyk naukovykh prats IPME im. H. Ye. Pukhova NAN Ukrainy, 57, 267–275 (in Ukrainian).
5. Sabat, V. I. (2004). Metody zakhystu dokumentiv v systemakh dokumentooborotu: Komp'iuterni tekhnolohii drukarstva, 12, 297–305 (in Ukrainian).
6. Durniak, B. V., Sabat, V. I., & Shvedova, L. Ye. (2011). Zahalna orhanizatsiia vykorystannia informatsiinykh zasobiv dlia stvorennia systemy upravlinnia povnovazhenniamy: Zb. nauk. pr. IPME NAN Ukrainy, 59, 200–207 (in Ukrainian).
7. Hutsaliuk, M. V. (2005). Identyfikatsiia fizychnykh osib yak protydiia orhanizovanii zlochynnosti ta teroryzmu: Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka). Kyiv, 11, 36–48 (in Ukrainian).

doi: 10.32403/1998-6912-2020-2-61-68-74

DEVELOPMENT OF ACCESS CONTROL SYSTEM TO DOCUMENTS IN ADMS FOR PUBLISHING HOUSES

V. I. Sabat, V. V. Matsyuk, M. M. Musijovska N. I. Kanevska

Ukrainian Academy of Printing,
19, Pid Holoskom St., Lviv, 79020, Ukraine
v_sabat@ukr.net

The basic means of access control to electronic documents are analysed, on the basis of which the system of access control in automated document management systems (ADMS) for publishing houses is offered.

The work on creating a system for document access control at a publishing house can be divided into three main areas: 1) the organization of work with documents and information contained in them; 2) the development of means of identification for all users of ADMS and methods of granting them certain powers; 3) ensuring the monitoring of the work of ADMS by the relevant security services. All areas of work with documents must be agreed in advance and prescribed in the security policy of the organization in the form of procedures for working with documents – from the beginning of their creation, working with them and to further destruction or archiving.

The organization of work with documents begins at the stage of their creation, when the classified information contained in the documents is determined and in accordance with it, each document is given a certain level of secrecy in the accompanying information to the document. The security services apply a certain level of protection to each document according to its level of secrecy. This process is carried out using the tools and procedures provided in the security policy of the organization (passwords, encryption, digital signature, etc.).

The development of methods and means of identifying users of the organization begins with the creation of a new user profile in the document access control system. In accordance with the powers granted, users in the security system are granted a certain level of access to documents. All users of ADMS should be acquainted with the rules of work with documents and with the duties and responsibilities in case of their violations.

Security services develop databases for documents and users, rules for user identification and authentication in ADMS and procedures for granting each entity of a publishing house a level of access to documents according to their level of secrecy. In the process of functioning of the publishing house, the security and access to documents services should systematically monitor the ADMS protection system for the presence of vulnerabilities and develop a strategy for the prompt resumption of its work in case of incidents.

Keywords: *document access control systems, automated document management systems, methods of identification and authentication of a person.*

Стаття надійшла до редакції 04.11.2020.
Received 04.11.2020.